

Basic Panorama Configuration

Version 1.2



Agenda

- Overview
- Setup
- High Availability
- Firewall Management
- Device Groups
- Templates and Template Stacks
- Log Collectors
- Plugins
- Device Deployment
- Resources
- Questions?

Assumptions

- You have a basic understanding of Palo Alto product offerings
- You have a basic understanding of firewall configuration and management
- You have a basic understanding of security
- You have a basic understanding of networking

Overview

Overview

Panorama:

- Virtual Machine or Appliance (M-Series)
 - M-300
 - M-700
- Licensing for 25, 100, or 1000 devices
- Support required (recurring cost)



Overview

Panorama Information:

- Plan your Panorama deployment strategy. [Document](#)
- Panorama must be the same version or higher than the highest PANOS device you wish to manage. Panorama can support older PANOS versions
- Panorama must have support to receive updates and patches
- Verify Panorama will manage all your firewall versions
- Estimate log storage capacity

11.2

11.2

11.1

10.2

10.1

Overview

Panorama Functions:

- Centralized configuration and deployment
- Aggregated logging with central oversight for reporting and analysis
- Distributed Administration

Panorama Models:

- Panorama mode (management and logging)
- Management-Only mode
- Log collector mode

Overview

Icons:

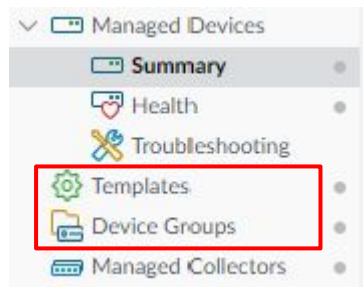


Overridden from Panorama



Inherited from Panorama

Overview



Setup

Setup

Panorama VM Setup:

- [System Requirements](#)
- [Install the VM](#) on your hypervisor or cloud
- Perform management interface configuration

```
> configure
# set deviceconfig system ip-address <Panorama-IP> netmask <netmask> default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
# commit
# exit
```

- Configure other settings - Panorama -> Setup -> Management
- Add logging capacity as necessary
- Configure the required mode (default: [Panorama Mode](#))
- Activate the license
- Update software and content updates
- Configure admin access

High Availability

High Availability

Prerequisites:

- Same form factor
- Same mode
- Same PANOS version
- Same set of license
- Virtual Panorama only
 - Virtual Appliance resources
 - Unique Serial Number
 - FIPCS-CC-Mode

It is recommended to match the logging capacity of HA Panoramas but not required.

High Availability

HA Configuration:

- Have one configured Panorama device and a peer with at least management configuration.
- Verify connectivity between Panorama management interfaces among peers as this is how synchronization is performed.



High Availability

HA Configuration: Setup

Setup

☒ Enable HA

Peer HA IP Address 192.168.12.25

Peer HA Serial 093248543012

☒ Encryption Enabled

Monitor Hold Time 3000

OK Cancel

milliseconds

Secondary peer IP Address and serial number

Encryption requires you to export an HA Key to the peer.
This is done in Panorama -> Certificate Management -> Certificates

Export Certificate Import HA Key Export HA Key

High Availability

HA Configuration: Priority

Election Settings 

Priority

Preemptive ☒

HA Timer Settings Recommended

Election Settings 

Priority primary

☒ Preemptive

HA Timer Settings Recommended

OK Cancel

None
primary
secondary
Recommended
Aggressive
Advanced

High Availability

HA Configuration: Path Monitoring

Path Monitoring

Enabled

☒

Failure Condition

any

Path Group

☐	NAME	ENABLED	GROUP FAILURE CONDITION	PING INTERVAL	PING COUNT	DESTINATION IP
--------------------------	------	---------	-------------------------	---------------	------------	----------------

+

Add

-

Delete

High Availability

HA Configuration: Path Monitoring (Cont.)

Path Group ?

Name

Google DNS

☒ Enabled

Failure Condition

☐ Any ☒ All

Ping Interval

5000

Ping Count

3

2 items

→

×

DESTINATION IP

8.8.8.8

4.2.2.2

+

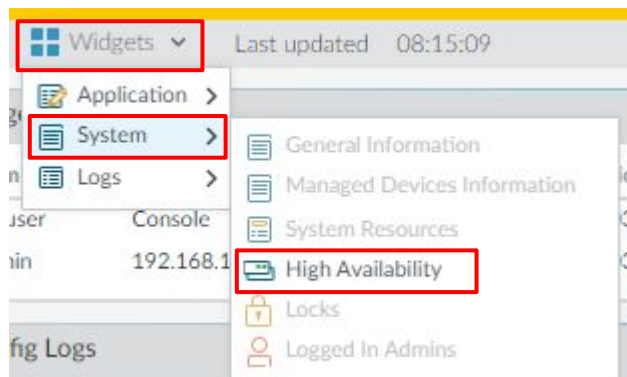
 Add

-

 Delete

High Availability

- Commit changes to primary peer
- Repeat the above steps to the secondary peer
 - Settings must match except:
 - IP address and serial number will be of the primary peer
 - Commit changes to peer
- On the Dashboard, create an HA widget to monitor



Firewall Management

Firewall Management

Configure firewall for basic management

- IP Address, subnet mask, default-gateway of management interface

Create the Device Auth Key - Panorama -> Device Registration Auth Key -> Add

Device Registration Auth Key ?

Name

Lifetime Days Hours Minutes
Ranges from 5 to 525600 mins.

Count

Device Type Any
Firewall
Log Collector

Devices

Devices this key is valid to use with

Please enter one or more device serial numbers. Enter one entry per row, separating the rows with a newline.

Firewall Management

Click OK and copy the key.

Authentication Key for Copying



Auth key

2:2
Ho
U2



U
W

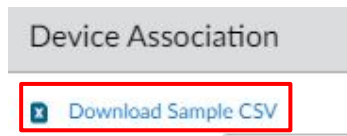
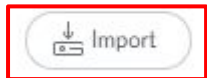
Copy Auth Key

Close

Firewall Management

Add firewalls to Panorama: Panorama -> Managed Devices -> Summary

- Manually add or bulk add with CSV
- To add with a CSV, click Add at the bottom. On the Add Device window, click import. On the Device Association window, click Download Sample CSV.



Firewall Management

Manually add firewalls: Click Add at the bottom

Add Device?

Serial

Please enter one or more device serial numbers. Enter one entry per row, separating the rows with a newline.

☒ Associate Devices

Device registration auth key is required for on-boarding firewall running PAN-OS 10.1 and above. All firewalls running PAN-OS 10.0 and lower do not require or support device registration auth key. You can use the button below to create OR copy the default auth key valid for 24 hours for any firewall you onboard OR go to Panorama->Device Registration Auth Key node to create OR copy auth keys with custom settings.

Generate Auth Key

Import

OK

Cancel

Add serial numbers of devices to import.

Optional to associate devices with device group, template, log collector/group when device is added. Do not use if devices are already configured.

Generate a new key or paste the one you created earlier

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto
NETWORKS

Firewall Management

Device Association:

Device Association?

[Download Sample CSV](#)

Select or drag and drop a CSV file to import

[Browse...](#) Clear

2 items

☐	SERIAL	DEVICE GROUP	TEMPLATE STACK	COLLECTOR GROUP	LOG COLLECTOR	AUTO PUSH ON 1ST CONNECT	TO SW VERSION
☐		dg_1	ts_1	default		☒	10.0.0
☒		dg_2	ts_2 ts_1	default		☒	

Firewall Management

Configure the firewall to communicate with Panorama:

On the firewall, go to Device -> Management -> Setup -> Panorama Settings

Panorama Settings



Firewall Management

Panorama Settings ?

Managed By ☒ Panorama ☐ Cloud Service

Panorama Servers

Auth key

☒ Enable pushing device monitoring data to Panorama

Receive Timeout for Connection to Panorama (sec)

Send Timeout for Connection to Panorama (sec)

Retry Count for SSL Send to Panorama

☒ Enable automated commit recovery

Number of attempts to check for Panorama connectivity

Interval between retries (sec)

Disable Panorama Policy and Objects

Disable Device and Network Template

OK

Cancel

Primary Panorama Server
Secondary Panorama Server

Auth key used when devices
were added to Panorama above

Firewall Management

Verify devices are connected: Panorama -> Managed Devices -> Summary

PANORAMA

DASHBOARD ACC MONITOR Device Groups POLICIES OBJECTS Templates NETWORK DEVICE PANORAMA

Panorama

Setup
High Availability
Config Audit
Managed WildFire Clusters
Managed WildFire Appliances
Password Profiles
Administrators
Admin Roles
Access Domain
Authentication Profile
Authentication Sequence
User Identification
Data Redistribution
Device Quarantine
Managed Devices
Summary
Health

dg_1 (2/2 Devices Connected): Shared > dg_1

	DEVICE NAME	VIRTUAL SYSTEM	MODEL	T...	SERIAL NUMBER	IP Address		I...	V...	TEMPLATE	DEVICE STATE
						IPV4					
☐	PA-3260-1		PA-3260					C...		ts_1	Connected
☐	PA-3260-2		PA-3260					C...		ts_1	Connected

Firewall Management

Import a configured device into Panorama: [Documentation](#)

- Get a device key
- Add the firewall
- Configure the firewall for Panorama management
- Export the configuration from the firewall
- Import the device configuration
- Commit changes to Panorama
- Push the configuration bundle to the firewall
- Push device group and templates to the device
- Verify synchronization

Firewall Management

Zero Touch Provisioning: [Documentation](#)

- Zero Touch Provisioning (ZTP) is designed to simplify and automate the onboarding of new firewalls to the Panorama™ management server. ZTP streamlines the initial firewall deployment process by allowing network administrators to ship managed firewalls directly to their branches and automatically add the firewall to the Panorama™ management server after the ZTP firewall successfully connects to the Palo Alto Networks ZTP service. This allows businesses to save on time and resources when deploying new firewalls at branch locations by removing the need for IT administrators to manually provision the new managed firewall. After successful on-boarding, Panorama provides the means to configure and manage your ZTP configuration and firewalls.
- ZTP is supported on the following ZTP firewalls:
 - PA-400 Series Firewalls
 - PA-820-ZTP and PA-850-ZTP
 - PA-1400 Series Firewalls
 - PA-3220-ZTP, PA-3250-ZTP, and PA-3260-ZTP
 - PA-3400 Series Firewalls
 - PA-5400 Series Firewalls
 - PA-5450

Device Groups

Device Groups

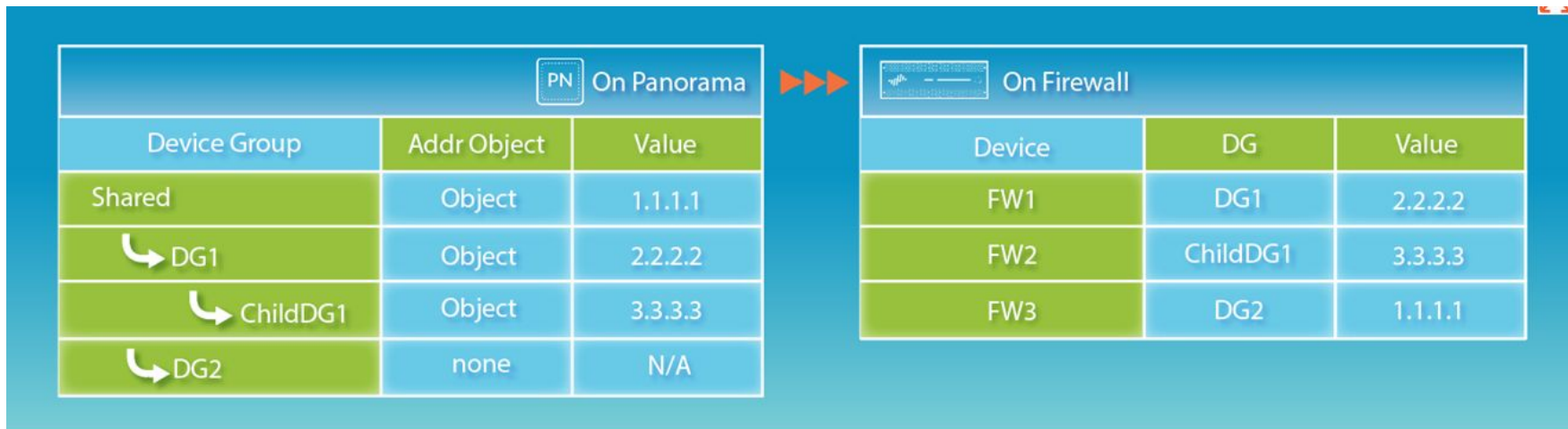
Device Groups



☐	NAME ^	DESCRIPTION
☐	▼  Shared	
☐	 SD-WAN_Branch	Device Group for SD-WAN branch configurations.
☐	 SD-WAN_Hub	Device Group for SD-WAN hub device configurations.

Device Groups

Managing Precedence:



Device Groups

Create New Device Group

Device Group ?

Name **New-DG**

Description **Recommended**

Parent Device Group **Shared**

Devices

FILTERS

- ☐ Device State
 - ☐ Platforms
 - ☐ Templates
 - ☐ Tags
 - ☐ HA Cluster ID
 - ☐ HA Cluster State
 - ☐ HA Pair Status

NAME

Add Firewalls to DG

Select All Deselect All ☐ Group HA Peers ☐ Filter Selected (0)

☒ User ID Master Device ☐ Cloud Identity Engine

None

The master device is the firewall from which Panorama gathers user ID information for use in policies.

☐ **REFERENCE TEMPLATES**

+ Add **-** Delete

If a DG requires a template, link them here.

Device Groups

Policies: Security

The screenshot shows the Palo Alto Networks Panorama interface. The top navigation bar includes 'PANORAMA', 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES' (selected), and 'OBJECTS'. Below this, there are tabs for 'Device Groups' and 'Templates'. The 'Device Groups' tab is active, and the 'Device Group' dropdown is set to 'SD-WAN_Hub'. The left sidebar shows the 'Security' policy selected, with 'Pre Rules' highlighted. The main table lists rules, with the first rule 'Known-Bad-EDL-Inbound' highlighted in tan. A green arrow points to this rule with a text annotation.

	NAME	LOCATION	TAGS	TYPE	ZONE	ADDRESS
1	Known-Bad-EDL-Inbound	Shared	none	universal	any	Palo Alto Netw...

Shaded tan because it is inherited
from a level above this one

Device Groups

Policies: Security

The screenshot shows the Palo Alto Networks Panorama interface. The top navigation bar includes 'PANORAMA', 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES' (highlighted), and 'OBJECTS'. Below this, the 'Device Groups' section is active, showing a dropdown for 'SD-WAN_Hub'. The left sidebar lists 'Security' (with 'Post Rules' selected), 'NAT', and 'QoS'. The main table displays the following data:

		NAME	LOCATION	TAGS	TYPE	Source			
						ZONE	ADDRESS	USER	DEVICE
1	SD-WAN BGP Traffic	SD-WAN_Hub	zone-internal zone-to-branc...	interzone	zone-Inter...	any	any	any	
2	Allow USER-ID traffi...	SD-WAN_Hub	zone-to-branc...	universal	zone-to-br...	any	any	any	

Normal blue tint is managed at this level

Device Groups

Panorama: Rule Processing Order:

The evaluation order of the rules is:



Device Groups

Policies: NAT

Device Group SD-WAN_Hub										
	NAME	LOCATION	TAGS	Original Packet						Translate
				SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION
1	ISP-1-NAT-Hub	SD-WAN_Hub	none	 gp-clients  inside	 outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 \$eth_1-1
2	ISP-2-NAT-Hub	SD-WAN_Hub	none	 gp-clients  inside	 outside	ethernet1/2	any	any	any	dynamic-ip-and-port ethernet1/2 \$eth_1-2

Device Groups

Objects:

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICES PANORAMA			
Device Group SD-WAN_Hub ▾			
Q			
	NAME	LOCATION	TYPE
☐	GP-Clients-GW1	SD-WAN_Hub	IP Netmask
☐	GP-Clients-GW2	SD-WAN_Hub	IP Netmask
☐	LAB-DC	SD-WAN_Hub	IP Netmask
☐	Asheville-LAN	Shared	IP Netmask
☐	Asheville-WAN	Shared	IP Netmask
☐	Denver-LAN	Shared	IP Netmask

Device Groups

Create a new object: Address

Address

Name

FS01

☐ Shared

☐ Disable override

Description

File Server

Type

IP Netmask

10.0.4.30

Resolve

Tags

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

OK

Cancel

Make Object reside in the Shared folder

Disable the ability for someone to override this object at a lower level

Device Groups

Moving between Device Groups:

Select the item to be moved and select  at the bottom of the page.

Move

Selected Objects

NAME	LOCATION
LAB-DC	SD-WAN_Hub

Destination

Shared

☒ Error out on first detected error in validation

Shared

SD-WAN_Branch

SD-WAN_Hub

Other Device Groups

Device Groups

Preview Rules to be pushed to a device: Select  Preview Rules at the bottom of the page

Combined Rules Preview ? ×								
Rulebase:	Security	Device Group:	SD-WAN_Hub	Device:	Jackson-FW	→		
NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
Known-Bad-EDL-Inb...	Block-Rules	universal	any	 Palo Alto Netw...	any	any	any	any
				 Palo Alto Netw...				
				 Palo Alto Netw...				
				 Palo Alto Netw...				
Known-Bad-EDL-Ou...	Block-Rules	universal	any	any	any	any	any	 Palo Alto Net
								 Palo Alto Net
								 Palo Alto Net
								 Palo Alto Net
Known-Bad-Countri...	Block-Rules	universal	any	 CN	any	any	any	any
				 IR				
Audit Comment Archive Reset Rule Hit Counter ▾  PDF/CSV								

Device Groups

Selecting a rule target:

When creating a new rule, you can choose the target for the rule inside a device group.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | **Target**

☒ Any (target to all devices)

Devices | Tags

FILTERS

- Device State
 - Connected (2)
- Platforms
 - PA-VM (2)
- Device Groups
 - SD-WAN_Branch (2)
- Templates
 - branch-stack (2)
- Tags
 - HA Cluster ID
- HA Cluster State
 - cluster-unknown (2)
- HA Pair Status

NAME

☒ SD-WAN_Branch	
☐ Asheville-FW	
☐ Denver-FW	

Select All Deselect All ☐ Group HA Peers

☐ Target to all but these specified devices and tags

Best Practice when targeting rules is to use audit comments for tracking. See next slide for enforcement.

Security Policy Rule

General | Source | Destination | Application | Service/URL

Name

Rule Type universal (default)

Description

Tags

Group Rules By Tag None

Audit Comment

[Audit Comment Archive](#)

Device Groups

Enforce audit comments: Panorama -> Setup -> Management

Policy Rulebase Settings

Require Tag on policies ☐

Require description on policies ☐

Fail commit if policies have no tags or description ☐

Require audit comment on policies ☐

Audit Comment Regular Expression

Policy Rule Hit Count ☒

Policy Application Usage ☒

Templates and Template Stacks

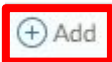
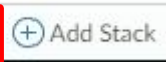
Templates and Template Stacks



☐	NAME	DESCRIPTION	TYPE	STACK
☐	iron-skillet	Iron Skillet Day 1 Configuration template	template	
☐	hub-template	Template for SD-WAN hub devices network configurations.	template	
☐	branch-template	Template for SD-WAN branch devices network configurations.	template	
☐	hub-stack		template-stack	iron-skillet hub-template
☐	branch-stack		template-stack	iron-skillet branch-template

Templates and Template Stacks

Create a new template: Panorama -> Templates

Click Add at the bottom of the page  

Template 

Name

New-Template

Description

OK

Cancel

Templates and Template Stacks

Create a new template stack: Panorama -> Templates

Click Add Stack at the bottom of the page

A screenshot of the 'Template Stack' configuration page in the Palo Alto Networks Panorama interface. The page has a light gray header with the title 'Template Stack' and a help icon. Below the header, there is a 'Name' field with the text 'New-Template-Stack' and a 'Description' field. A checkbox labeled 'Automatically push content when software device (vm or container) registers to Panorama' is present. The 'Devices' section contains a 'FILTERS' sidebar with checkboxes for 'Platforms', 'Device Groups', 'Tags', 'HA Cluster ID', 'HA Cluster State', and 'HA Pair Status'. A search bar with '0 items' and a close icon is next to the filters. Below the filters, there are buttons for 'Select All', 'Deselect All', and a checkbox for 'Group HA Peers', followed by a 'Filter Selected (0)' checkbox. The 'User ID Master Device' section has a radio button for 'User ID Master Device' (selected) and a radio button for 'Cloud Identity Engine', with a dropdown menu showing 'None'. A note explains that the master device is the firewall from which Panorama gathers user ID information. The 'TEMPLATES' section is a list with a plus icon, the text 'TEMPLATES', and buttons for 'Add', 'Delete', 'Move Up', and 'Move Down'. A note states that the template at the top of the stack has the highest priority. The 'Select Devices' and 'Select Templates' text is overlaid in purple on the respective sections, and both sections are highlighted with red rectangular boxes.

Templates and Template Stacks

Templates Order of Precedence:

☐	TEMPLATES
☐	admin_config
☐	TPL
☐	K8S-Network-Setup
☐	TPL-2
+ Add − Delete ↑ Move Up ↓ Move Down	

The Template at the top of the Stack has the highest priority in the presence of overlapping config

Templates and Template Stacks

Template and Template Stack Variables:

To enable you to more easily reuse templates or template stacks, you can use template and template stack variables to replace IP addresses, Group IDs, and interfaces in your configurations. Template variables are defined at either the template or template stack level and you can use variables to replace IP addresses, IP ranges, FQDN, interfaces in IKE, VPN and HA configurations, and group IDs.

- All variable names must start with a \$.
 - Example: \$pri-isp-ip
- Template stack variables override a template variable

Templates and Template Stacks

Manage Variables: Panorama -> Templates

VARIABLES	DEVICE KEY-VALUE TABLE
Manage...	
Manage...	
Manage...	
Manage...	View
Manage...	View

Template Variables

0 items

→

×

☐	NAME	TYPE	VALUE	DESCRIPTION

+

Add

-

Delete

↺

Clone

Templates and Template Stacks

Create a new variable:

Variable ?

Name

Variables need to begin with '\$'

Type

Description

- IP Netmask
- IP Range
- FQDN
- Group ID
- Device Priority
- Device ID
- Interface
- As Number
- Qos Profile
- Egress Max
- Link Tag

Variable ?

Name

Variables need to begin with '\$'

Type

Description

Templates and Template Stacks

Template Variables CSV:

A	B	C	D
variable_name	variable_type	unknown/0079	unknown/0079
\$isp_def-gw-1	ip-netmask	10.5.0.1	10.6.0.1
\$eth_1-1	ip-netmask	10.5.0.2/30	10.6.0.2/30
\$eth_1-2	ip-netmask	10.5.1.2/30	10.6.1.2/30
\$eth_1-3	ip-netmask	172.16.34.1/24	172.16.36.1/24
\$isp_def-gw-2	ip-netmask	10.5.1.1	10.6.1.1
\$local_subnet	ip-netmask	172.16.34.0/24	172.16.36.0/24
\$peer_subnet	ip-netmask	172.16.32.0/24	172.16.32.0/24
\$LAB-DC01	ip-netmask	#inherited#	#inherited#

CSV File (Export)

KEY NAME	DENVER-FW (007954000341...	ASHEVILLE-FW (007954000342...
\$isp_def-gw-1	10.5.0.1	10.6.0.1
\$eth_1-1	10.5.0.2/30	10.6.0.2/30
\$eth_1-2	10.5.1.2/30	10.6.1.2/30
\$eth_1-3	172.16.34.1/24	172.16.36.1/24
\$isp_def-gw-2	10.5.1.1	10.6.1.1
\$local_subnet	172.16.34.0/24	172.16.36.0/24
\$peer_subnet	172.16.32.0/24	172.16.32.0/24
\$LAB-DC01	172.16.32.25	172.16.32.25

Device Key-Value Table

Templates and Template Stacks

Edit Variables in UI: Panorama -> Managed Devices -> Summary

	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address		HA	VARIABLES
						IPV4	IPV6	CLUSTER STATE	
SD-WAN_Branch (2/2 Devices Connected): Shared > SD-WAN_Branch									
☐	Denver-FW		PA-VM		007954000341864	192.168.18.32		cluster-unknown	Edit
☐	Asheville-FW		PA-VM		007954000342117	192.168.18.33		cluster-unknown	Edit
SD-WAN_Hub (1/1 Devices Connected): Shared > SD-WAN_Hub									
☐	Jackson-FW		PA-VM		007954000341888	192.168.18.31		cluster-unknown	Edit

Templates and Template Stacks

Edit Variables in UI:

Template Variables for Device Denver-FW ?

Device Name Denver-FW

Template Stack branch-stack

☐	NAME		TEMPLATE	TYPE	VALUE
☐	\$isp_def-gw-1		Overridden on device	IP Netmask	10.5.0.1
☐	\$eth_1-1		Overridden on device	IP Netmask	10.5.0.2/30
☐	\$eth_1-2	✓	Overridden on device	IP Netmask	10.5.1.2/30
☐	\$eth_1-3		Overridden on device	IP Netmask	172.16.34.1/24
☐	\$isp_def-gw-2		Overridden on device	IP Netmask	10.5.1.1
☐	\$local_subnet		Overridden on device	IP Netmask	172.16.34.0/24
☐	\$peer_subnet		Overridden on device	IP Netmask	172.16.32.0/24
☐	\$LAB-DC01		branch-template	IP Netmask	172.16.32.25

8 items → ×

⊖ Delete Override Revert Get values used on device

Template variables can be overridden if inherited from the template

Log Collectors

Log Collectors

To save logs to Panorama, you need to configure log collectors. These can be local or dedicated.

Panorama -> Setup -> Managed Collectors



Log Collectors

Collector



General

Authentication

Disks

Communication

Collector S/N

Collector Name

Inbound Certificate for Secure Syslog

None

Certificate for Secure Syslog

None

Panorama Server IP

Panorama Server IP 2

Domain

Primary DNS Server

Secondary DNS Server

Timezone

Latitude

Longitude

☐ Primary NTP Server

NTP Server Address

Authentication Type

None

☐ Secondary NTP Server

NTP Server Address

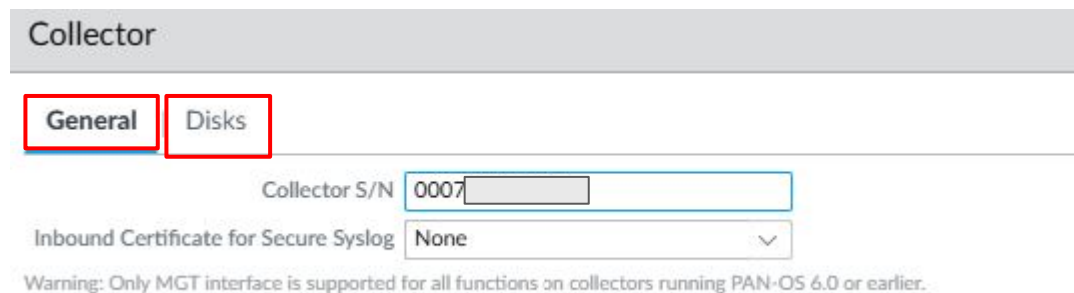
Authentication Type

None

Warning: Only MGT interface is supported for all functions on collectors running PAN-OS 6.0 or earlier.

Log Collectors

If Panorama is the collector (local), this is the configuration screen:



Collector

General Disks

Collector S/N 0007

Inbound Certificate for Secure Syslog None

Warning: Only MGT interface is supported for all functions on collectors running PAN-OS 6.0 or earlier.

Note: After you add the serial number, commit to Panorama. Then you can add logging disks.

Log Collectors

Check the Health Status to determine viability of Log Collector:

Configuration		Run Time		LOG REDISTRIB... STATE	LAST COMMIT STATE	CERTIFICA...	HEALTH	
STATUS	DETAIL	STATUS	DETAIL					
 In sync	none	connected	connected to all LCs in group	none	commit succeeded	pre-defined	 Health Status	Statistics

Health Status ?	
DATA POINTS	HEALTH STATUS
logd	
vldmgr	
vlds	
es	

Log Collectors

Log Collector Groups:

Log collector groups are used to create a logical unit of collector to collect logs from firewalls.

Panorama -> Setup -> Collector Groups

Log Collectors

Collector Group

General | Monitoring | Device Log Forwarding | Collector Log Forwarding | Audit

Name

Log Storage

Min Retention Period (days)

[1 - 2000]

Collector Group Members



COLLECTORS ^



Add



Delete

- ☐ Enable log redundancy across collectors
- ☐ Forward to all collectors in the preference list
- ☐ Enable secure inter LC Communication

Log Collectors

Collector Log Forwarding:

Log Settings

Name

Filter

All Logs

Description

Forward Method

☐

SNMP

^

+ Add

- Delete

☐

EMAIL

^

+ Add

- Delete

☐

SYSLOG

^

+ Add

- Delete

☐

HTTP

^

+ Add

- Delete

Panorama Plugins

Plugins

Panorama supports an extensible plugin architecture that enables the integration and configuration of the following capabilities: Panorama -> Plugins

- AIOps
- AWS
- Azure
- Cisco ACI
- Cisco TrustSec
- Cloud Services
- Enterprise Data Loss Prevention
- Google Cloud Platform
- Panorama Interconnect
- Nutanix
- SD-WAN
- VMware NSX
- VMware vCenter
- Zero Touch Provisioning
- IPS Signature Converter

Plugins

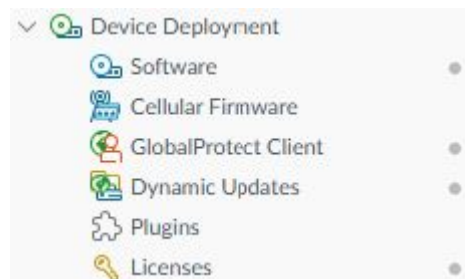
dlp							34 / 470
FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS	RELEASE NOTE URL
Name: dlp							
dlp-5.0.6	5.0.6	2025/03/19 21:00:22.276342	1M	✓	✓	Remove Config  Uninstall 	
Name: dlp-1.0.1							
dlp-1.0.1	1.0.1	2020/10/29 17:08:22	1M			Download 	Release Notes
Name: dlp-1.0.2							
dlp-1.0.2	1.0.2	2020/12/10 08:38:03	1M			Download 	Release Notes

 Check Now  Upload

Device Deployment

Device Deployment

Configure device deployment settings for firewalls:



Device Deployment

Software:

VERSION	FILE NAME	PLATFORM	SIZE	SHA256	RELEASE DATE	AVAILABLE	ACTION	DOCUMENTATION
11.2.9.aingfw	PanOSAINgfw_vm-11.2.9.aingfw	AI Runtime Security	1227 MB	da7d5197812e340d77b8e8...	2025/09/18 14:14:41		Download	Release Notes
11.2.9	PanOS_7000b-11.2.9	7000b	1101 MB	cc096909f716f3f97abdb95...	2025/09/18 14:01:12		Download	Release Notes
11.2.9	PanOS_vm-11.2.9	vm	781 MB	e737f3368bd9a96fcceb73a...	2025/09/18 14:01:08	Downloaded ☒	Validate Export Install	Release Notes
11.2.9	WildFire_m-11.2.9	m	364 MB	789150d548177259720bce...	2025/09/18 14:01:05		Download	Release Notes
11.2.9	Panorama_m-11.2.9	m	1074 MB	8cc7b95d5cd443c35cd2063...	2025/09/18 14:01:04		Download	Release Notes
11.2.9	PanOS_5400-11.2.9	5400	1129 MB	f4185675bef15109dba0360...	2025/09/18 14:01:00		Download	Release Notes
11.2.9	PanOS_3400-11.2.9	3400	1160 MB	48531cf510c7b6ffb053d70...	2025/09/18 14:00:56		Download	Release Notes
11.2.9	PanOS_5400f-11.2.9	5400f	1034 MB	b651ba41ce284a7fd89f9a5...	2025/09/18 14:00:52		Download	Release Notes



Device Deployment

Software:

Deploy Software file: PanOS_vm-11.2.9 ?

Filters

☐ Device State

☐ Connected (3)

☐ Platforms

☐ PA-VM (3)

☐ Device Groups

☐ SD-WAN_Branch (2)

☐ SD-WAN_Hub (1)

☐ Templates

☐ branch-stack (2)

☐ hub-stack (1)

☐ Tags

☐ HA Cluster ID

☐ HA Cluster State

☐ HA Pair Status

☐ Reboot device after install

Devices

3 items → ×

☐	DEVICE NAME	SERIAL NUMBER ^	CURRENT VERSION	HA PAIR STATUS
☐	West-VM	0079	11.2.8	
☐	East-FW	0079	11.2.8	
☐	DC-FW	0079	11.2.8	

☐ Group HA Peers ☐ Filter Selected (0)

OK

Cancel

Device Deployment

Licenses:

DEVICE	VIRTUAL SYSTEM	THREAT PREVENTION	URL	SUPPORT	GLOBALPROTECT GATEWAY	GLOBALPROTECT PORTAL	WILDFIRE	VM-SERIES CAPACITY	AUTOFOCUS	STRATA LOGGING SERVICE
West-VM	✓	✓ Expires: 3/27/2026	✓ PaloAlto Networks Expires: 3/27/2026	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 7/9/2026
East-FW	✓	✓ Expires: 3/27/2026	✓ PaloAlto Networks Expires: 3/27/2026	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 7/9/2026
DC-FW	✓	✓ Expires: 3/27/2026	✓ PaloAlto Networks Expires: 3/27/2026	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 7/9/2026

Resources

Resources

- [Panorama Administrator's Guide](#)
- [Panorama Home Page](#)
- [Panorama Best Practices Guide](#)
- [Panorama Compatibility Matrix](#)

Questions?

Thank You!

